Novel Algorithm for Secure User Authentication and Steganography

Jaya Tiwari[1], Vimal Kumar Agrawal[2]
[1]MTech.Scholar , [2]Associate Professor,
[1,2] Department of Electronics & Communication Engineering, , Apex Institute of Engineering and Technology, Jaipur ,India ,Rajasthan

Abstract : The requirement of the information technology age is to transfer the data in a secure way. The proposed work aims for the secure data transfer with using the novel concept of the encrypted image as password for the authentication of the users and also provided the encrypted text steganography on all types of carriers including the image , audio and also the video.

Index Terms: Steganography, Security ,Authentication.

I. Introduction

Steagnography offers discharge and secure method for correspondence. It has numerous application zones, for example, sound video synchronization, copyright control, TV broadcasting, in safeguard powers and digital watermarking and so forth. The watermarking, steganography and cryptography are interrelated [1]. Initial two methods are bit comparable yet cryptography is recognized from these two. In steganography, the mystery information or client data is disguised in another media that media could be picture, sound or video for example called spread media[2].

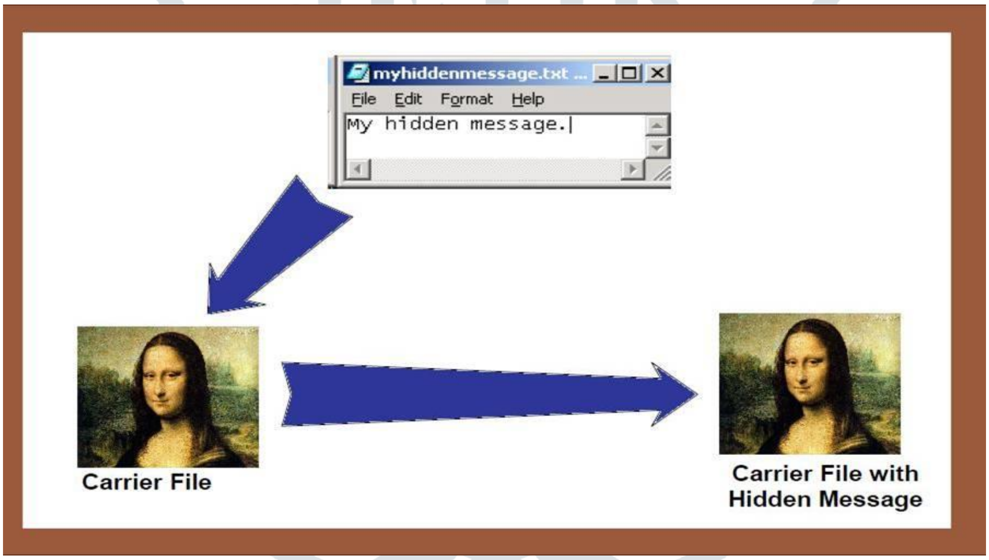


Fig 1 Stegnography Concept

Steganography is the craft of hiding information in manners that keeps the identification of concealed messages. Steganography incorporate a variety of mystery specialized strategies that conceal the message from being seen or found . In cryptography, the message or encoded message is implanted in a digital host before going it through the system, consequently the presence of the message is obscure. Other than hiding data for privacy, this methodology of information hiding can be stretched out to copyright insurance for digital media: sound, video and pictures. The developing potential outcomes of current interchanges need the uncommon methods for security particularly on PC organize. The system security is winding up progressively vital as the quantity of data being traded. on the web increase.[3]

II. Related Work

P Shaikh Shakeela, et. al ,2016 This paper proposes a basic and powerful strategy for sound data implanting into recordings. Vigor in this technique comes due to the utilization of twofold coding system. Here twofold coding methods utilizing two sorts of codes on similar data in a steady progression. Strength in this technique comes in view of the utilization of twofold coding component. Here twofold coding methods utilizing two sorts of codes on similar data in a steady progression. This gives greater security and dependability to the concealed data into video

Priyanka Sahute, et.al,2015 To make the security of information we are utilizing Secure Messaging utilizing Image Steganography. Any measure of data or archive can be effectively installed. On the off chance that any information is installed in stego picture and exchange to client with no unsettling influence of that spread picture and transitional individual can't understood that protected information. RSA Algorithm and HASH-LSB method has been utilized. In cryptography RSA Algorithm is utilized for Encryption and Decryption. RSA Algorithm having two methodologies: Asymmetric and Symmetric.

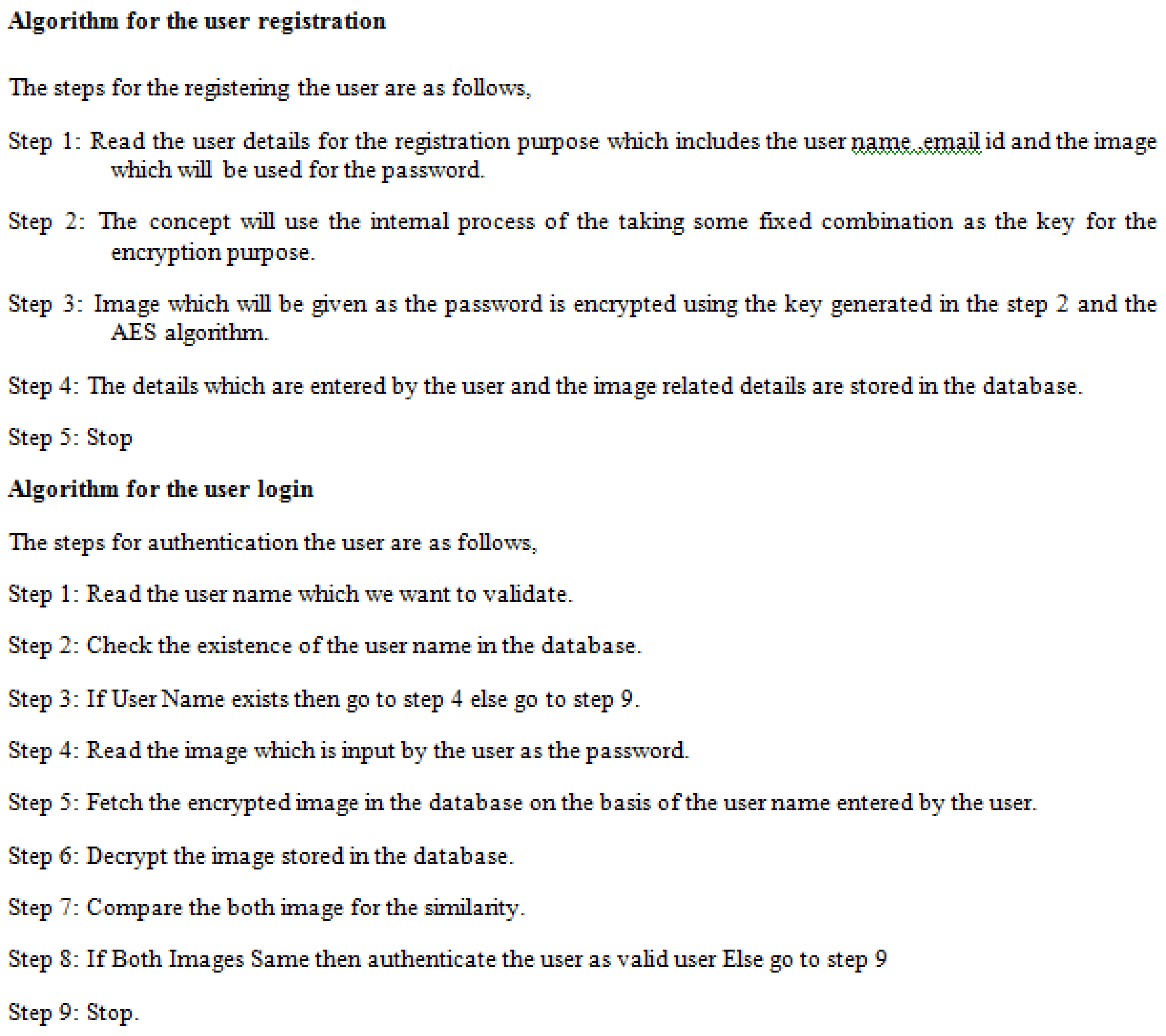
Pooja,Sandeep Toshniwal et. al 2017 The advancement enthusiasm of this strategy like in the use of video inquiries as spread, and express utilization of Frame-QR Code Randomization on along these lines factor parameters, for instance, customer choice progressively the thought novel and convincing. Moreover encryption of QR Code using VLMKG (Variable length mixed key Generation) cryptography totally Jeopardizes unapproved unraveling attempts. We attempted our proposed structure on a course of action of 2-3 QR Code and 2-3 video gathering and Found our and MATLAB utilization had sublimely scrutinized the proposed count and the results were seen to be tasteful.

III. PROBLEM STATEMENT

The problem statement which is being focused in the work which we have implemented is divided into the three segments. The first segment is focused on the proper authentication of the user. The concept of the authentication of the user is required which will be different from the normal alphanumeric concept of passwords. After the validation approach the next concept is to proceed for the secure data transfer in the steganographic way. The system then also proceeds for the three concepts, Image, Audio and video. Thus, for the work we have selected is to aim for the development of the system which handles all type of data and together with that also able to hide data in all types of carriers.

IV. PROPOSED WORK

The proposed work contains the algorithms related user authentication and steagnography



Algorithm for the user registration

The steps for the registering the user are as follows,

Step 1: Read the user details for the registration purpose which includes the user name ,email id and the image which will be used for the password.

Step 2: The concept will use the internal process of the taking some fixed combination as the key for the encryption purpose.

Step 3: Image which will be given as the password is encrypted using the key generated in the step 2 and the AES algorithm.

Step 4: The details which are entered by the user and the image related details are stored in the database.

Step 5: Stop

Algorithm for the user login

The steps for authentication the user are as follows,

Step 1: Read the user name which we want to validate.

Step 2: Check the existence of the user name in the database.

Step 3: If User Name exists then go to step 4 else go to step 9.

Step 4: Read the image which is input by the user as the password.

Step 5: Fetch the encrypted image in the database on the basis of the user name entered by the user.

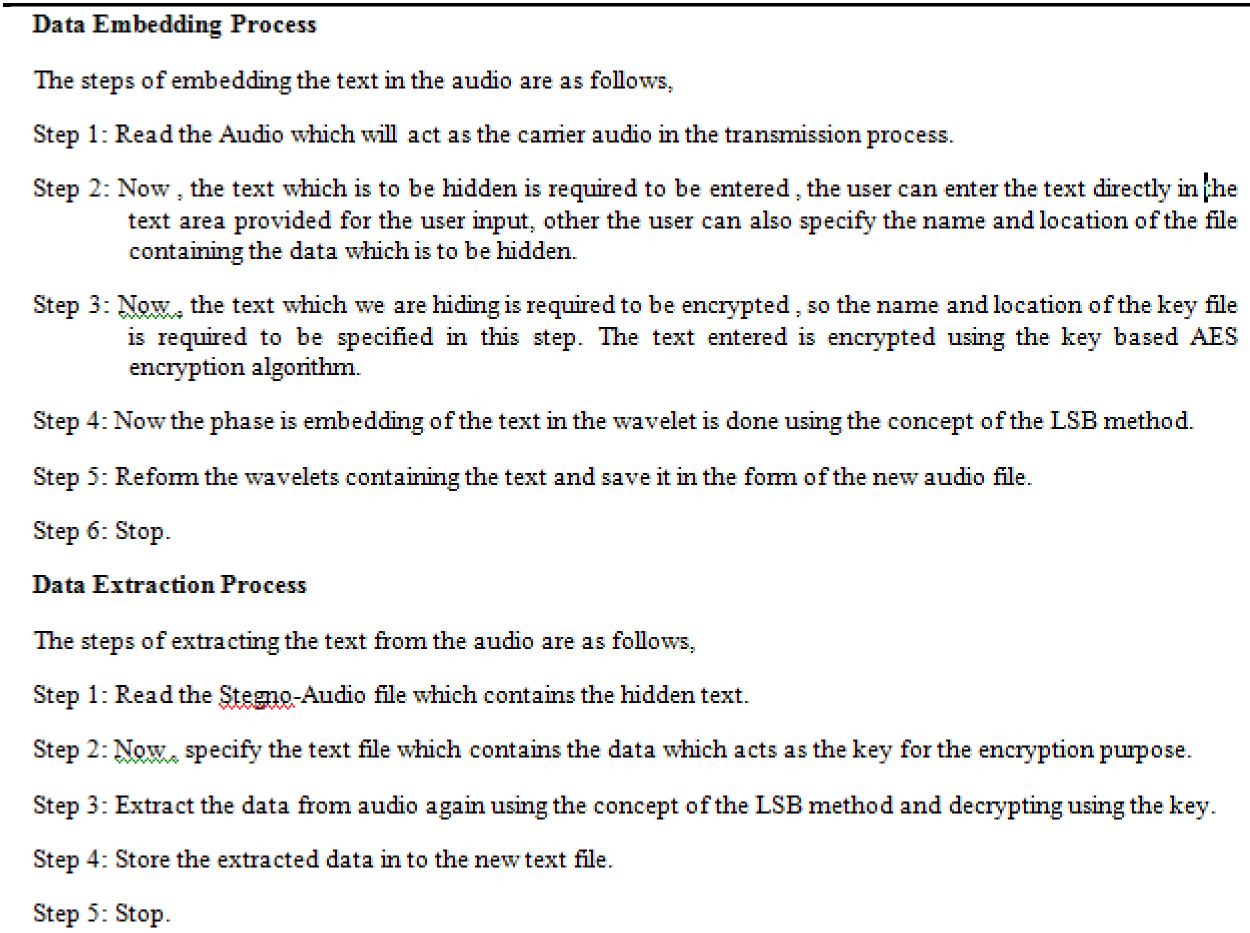
Step 6: Decrypt the image stored in the database.

Step 7: Compare the both image for the similarity.

Step 8: If Both Images Same then authenticate the user as valid user Else go to step 9

Step 9: Stop.

The next segment is the algorithms which are related for the steagnographic operation on the audio files , the algorithms are shown be ,



Data Embedding Process

The steps of embedding the text in the audio are as follows,

Step 1: Read the Audio which will act as the carrier audio in the transmission process.

Step 2: Now , the text which is to be hidden is required to be entered , the user can enter the text directly in the text area provided for the user input, other the user can also specify the name and location of the file containing the data which is to be hidden.

Step 3: Now , the text which we are hiding is required to be encrypted , so the name and location of the key file is required to be specified in this step. The text entered is encrypted using the key based AES encryption algorithm.

Step 4: Now the phase is embedding of the text in the wavelet is done using the concept of the LSB method.

Step 5: Reform the wavelets containing the text and save it in the form of the new audio file.

Step 6: Stop.

Data Extraction Process

The steps of extracting the text from the audio are as follows,

Step 1: Read the Stegno-Audio file which contains the hidden text.

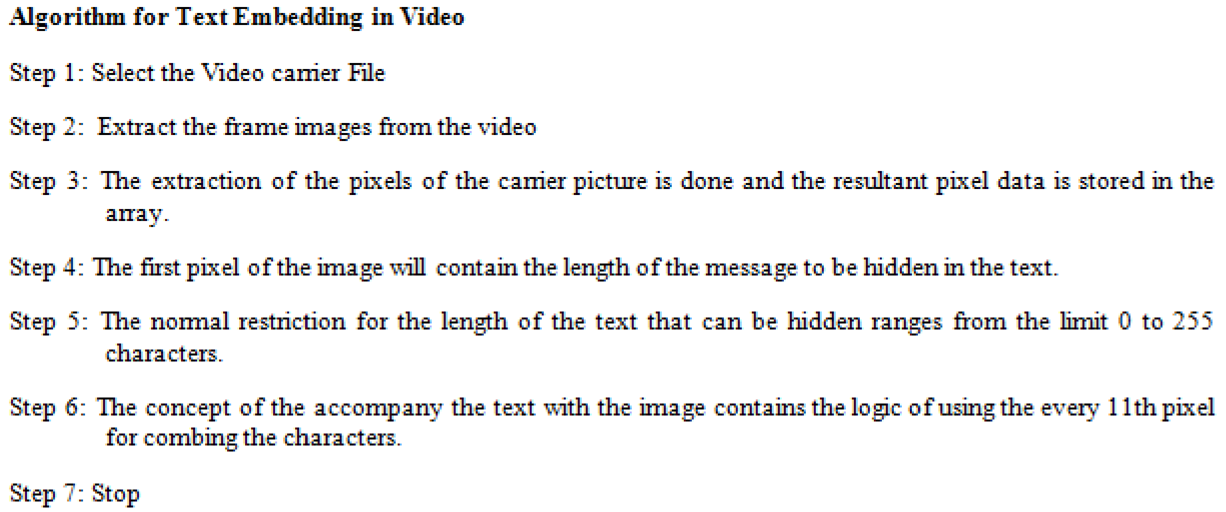
Step 2: Now , specify the text file which contains the data which acts as the key for the encryption purpose.

Step 3: Extract the data from audio again using the concept of the LSB method and decrypting using the key.

Step 4: Store the extracted data in to the new text file.

Step 5: Stop.

Now the next section will incorporate to the video based embedding and the extraction process and the algorithms which are related to that are written below.



Algorithm for Text Embedding in Video

Step 1: Select the Video carrier File

Step 2: Extract the frame images from the video

Step 3: The extraction of the pixels of the carrier picture is done and the resultant pixel data is stored in the array.

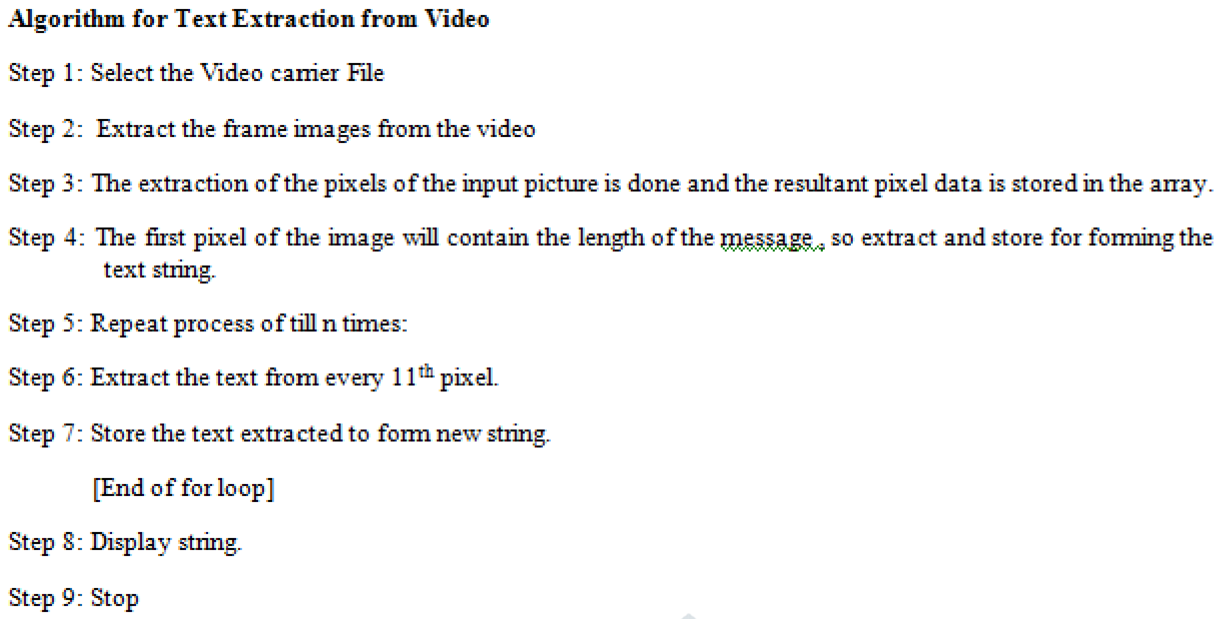
Step 4: The first pixel of the image will contain the length of the message to be hidden in the text.

Step 5: The normal restriction for the length of the text that can be hidden ranges from the limit 0 to 255 characters.

Step 6: The concept of the accompany the text with the image contains the logic of using the every 11th pixel for combing the characters.

Step 7: Stop

The processes after the embedding of the text in the video based file , the next segment of the algorithm will corresponds to the extraction of the text form the video based file.



Algorithm for Text Extraction from Video

```
Step 1: Select the Video carrier File
Step 2:  Extract the frame images from the video
Step 3: The extraction of the pixels of the input picture is done and the resultant pixel data is stored in the array.
Step 4: The first pixel of the image will contain the length of the message , so extract and store for forming the
        text string.
Step 5: Repeat process of till n times:
Step 6: Extract the text from every 11th pixel.
Step 7: Store the text extracted to form new string.
        [End of for loop]
Step 8: Display string.
Step 9: Stop
```

IV. RESULTS AND DISCUSSION

The quality of the proposed work lies on the extraordinary idea of giving the single stage to the every one of the transporters yet at the same time utilizing a few apparatuses and the quality checking alternatives we have tried the result based on the keys which are utilized in the idea proposed. The idea of the video steganography makes utilizing of MD5 Hash approval which makes the key more quality full.

The key utilized is

a@12_#7d9eb1458004307d5b3d2e0ff3071cb9

where ,

7d9eb1458004307d5b3d2e0ff3071cb9 is the MD5 hash of the shrouded content

Another testing site is comparitech.com

Secret key Strength : Excellent

Another devices is cryptool which look at the quality of the secret key.

Result Entropy: 2.84

V. Conclusion

The single platform for the proper security of user authentication and data transfer found to be effective as compared to the previous work done. As the single platform is not available for all the carriers and also the MD5 hash validations for the work validation also raised up the security.

References

[1] Palak R Patel, Yask Patel Survey2 on Different Methods of Image Steganography International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 2, Issue 12, December 2014.

[2] Anil Kumar *, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering © 2013, IJARCSSE All Rights Reserved Page | 363 ,Volume 3, Issue 7, July 2013

[3] Sahu, Suraj Kumar, and Sandeep Kumar Gonnade. "Encryption in QR Code Using Stegnography." International Journal of Engineering Research and Applications 3.4 (2013): 1738-1741.

[4] Shaikh Shakeela, P. Arulmozhivarman, Rohit Chudiwal, Samadrita Pal,"Double Coding Mechanism for Robust Audio Data Hiding in Videos",IEEE International Conference On Recent Trends In Electronics Information Communication Technology,2016

[5] Priyanka Sahute, Swati Waghamare, Supriya Patil,Ashwini Diwate,"Secure Messaging Using Image Stegnography",International Journal of Modern Trends in Engineering and Research,2015

[6] Pooja,Sandeep Toshniwal,"A QR Code Based Highly Secure Covert Communication",IEEE,2017

[7] Priyanka A. Singh, Prof. Leena H. Patil, Prof.Namrata.S.Mahakalkar "A Survey on Secret Image Sharing Using QR Code Generation Technique" IJLTET 2016.